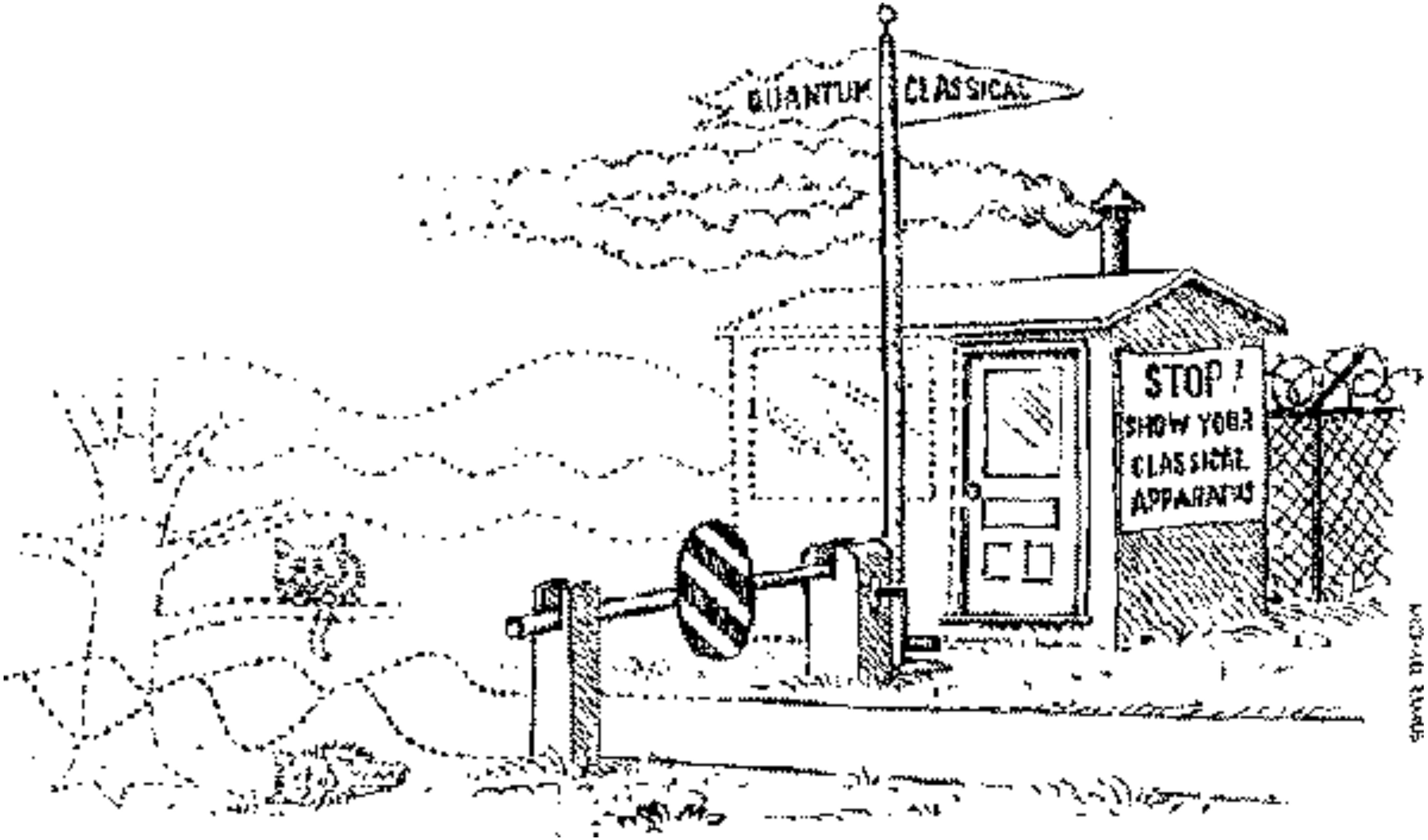
Quantum Computing



Information is Physical

information is always tied to a physical realization

fundamental limits:

speed-limit: c (relativity)

resetting a bit costs > $kT \ln 2$ (statisical mechanics

dynamical RAM represents bit by charge on capacitor:

Cbit

b=1 – capacitor charged

b=0 – capacitor uncharged

alternative: **represent bit by spin-½**

Qbit

$$| b\rangle = \alpha | 0\rangle + \beta | 1\rangle$$

superposition of (classical) bits

Rolf Landauer

Quantum Information

Qbits cannot be copied
(no-cloning theorem)

disadvantage:
information in Qbit not fully accessible
(uncertainty!)

advantage:
eavesdropping on a quantum channel detectable
$\Rightarrow$ quantum cryptography

No-Cloning Theorem

Wootters&Zurek Nature **299**, 802 (1982)

it is impossible to copy an *unknown* quantum state

proof by *reductio ad absurdum*

let U be unitary cloning operator: $U|\Psi\rangle|s\rangle = |\Psi\rangle|\Psi\rangle$ for *any* $|\Psi\rangle$

$$\text{then}\quad \langle s|\langle\Psi|U^\dagger \cdot U|\Phi\rangle|s\rangle \overset{\text{unitary}}{=} \underbrace{\langle s|s\rangle}_{=1}\langle\Psi|\Phi\rangle$$

$$\overset{\text{def}}{=} \langle\Psi|\langle\Psi| \cdot |\Phi\rangle|\Phi\rangle = \langle\Psi|\Phi\rangle^2$$

thus $\langle\Psi|\Phi\rangle^2 \overset{!}{=} \langle\Psi|\Phi\rangle$; only possible if $\langle\Psi|\Phi\rangle = 0$ or 1

$\Rightarrow$ only orthogonal basis states can be cloned

(reversible copying of Cbits)

quantum parallelism

$$U_H|0\rangle U_H|0\rangle \ldots U_H|0\rangle = U_H^{\otimes n}|00\ldots 0\rangle = \sum_x |\mathbf{x}\rangle$$

superposition of all 2^n basis states

implement classical function f(x) as unitary operator:

$$U_f|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|\mathbf{y} \oplus f(\mathbf{x})\rangle$$

then $$U_f U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_x |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_x \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}_{x \text{ and } f(x) \text{ entangled!}}$$

simultaneous evaluation of 2n function values

problem: only one (random!) *f(x)* can be measured

classical logics

Boolean operations

NOT gate

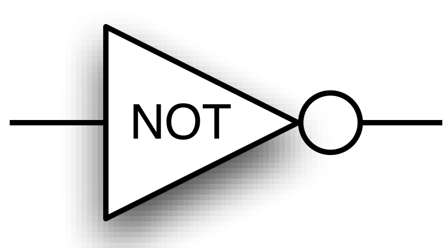
a	¬a
0	1
1	0

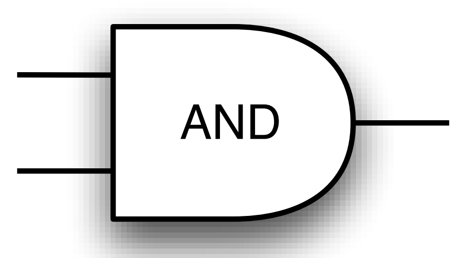
AND gate

a	b	$a \cdot b$
0	0	0
0	1	0
1	0	0
1	1	1

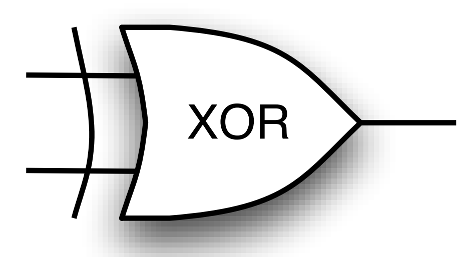
XOR gate

a	b	$a \oplus b$	a
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1





not reversible!

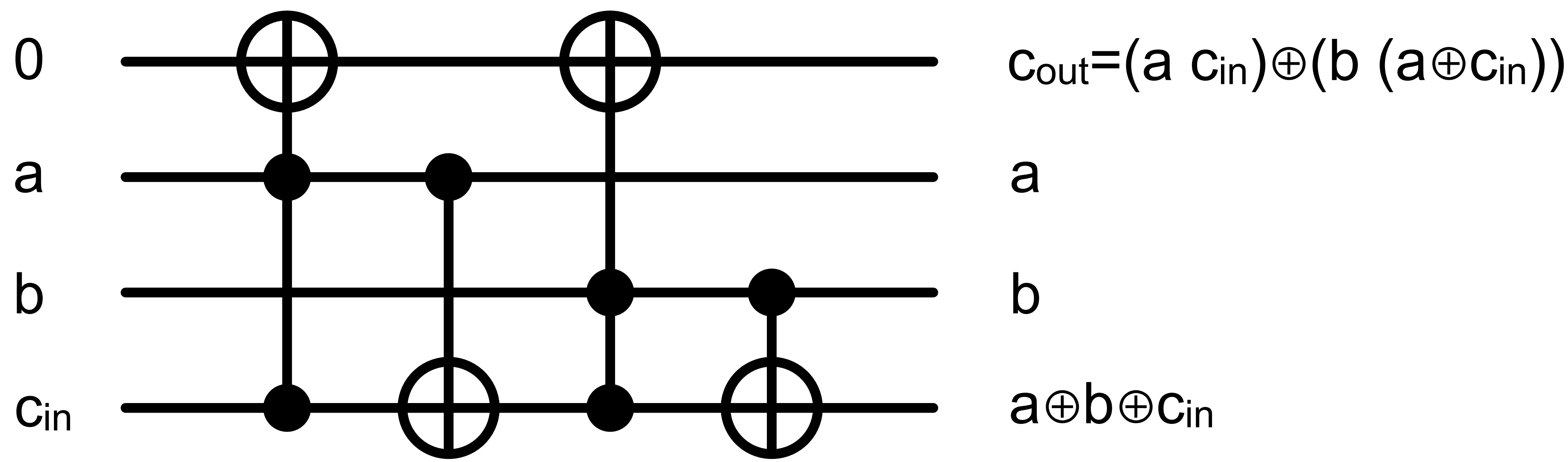


reversible: cNOT

reversible logics

e.g. controled NOT and Toffoli gates

example:
full adder



reversible gate defines operation on basis states
naturally extends to unitary operators

quantum gates without classical analogon:
e.g. Hadamard gate (creates superpositions)

$$U_H|0\rangle \quad = \quad \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$U_H|1\rangle \quad = \quad \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Quantum Computing

notion of computability unchanged
quantum systems can be simulated on a classical computer

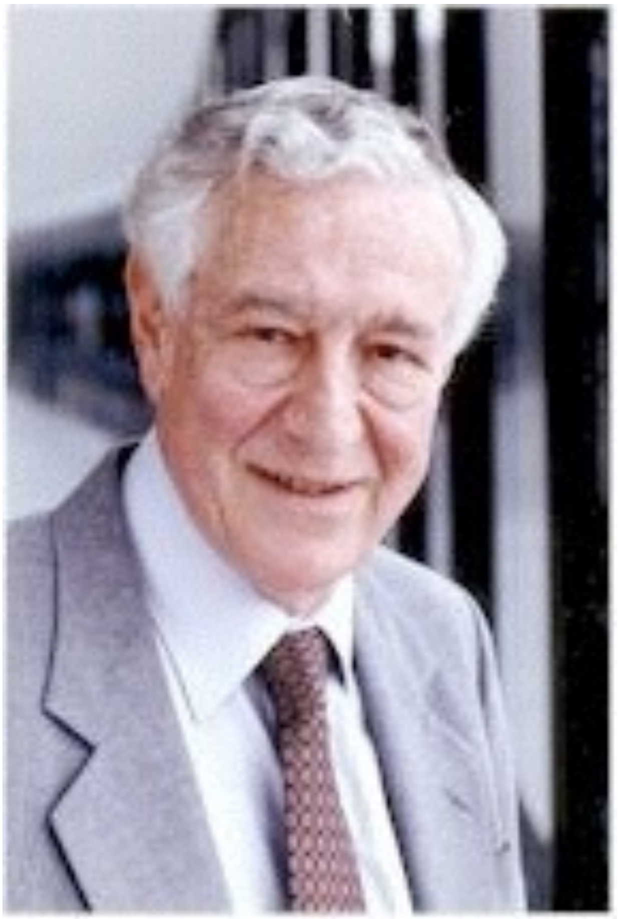
computational complexity reduced:
quantum computers can be much faster than classical ones

problem	classical algorithm	quantum algorithm
factoring N	number field sieve $O(e$	Shor algorithm:
unstructured search in N items	brute force: $O(N)$	Grover algorithm: $O(\sqrt{\ } N)$

Landauer’s Disclaimer

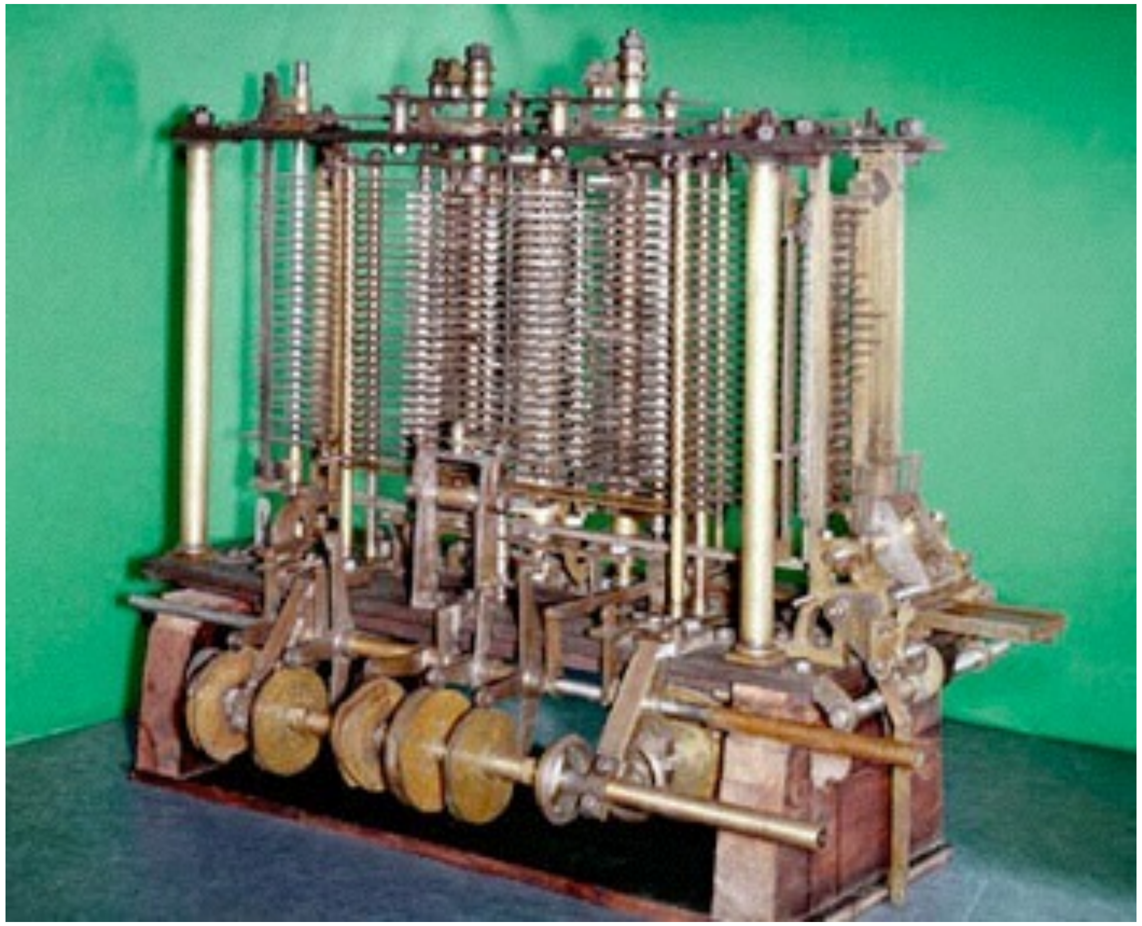
Nature **400**, 720 (1999)

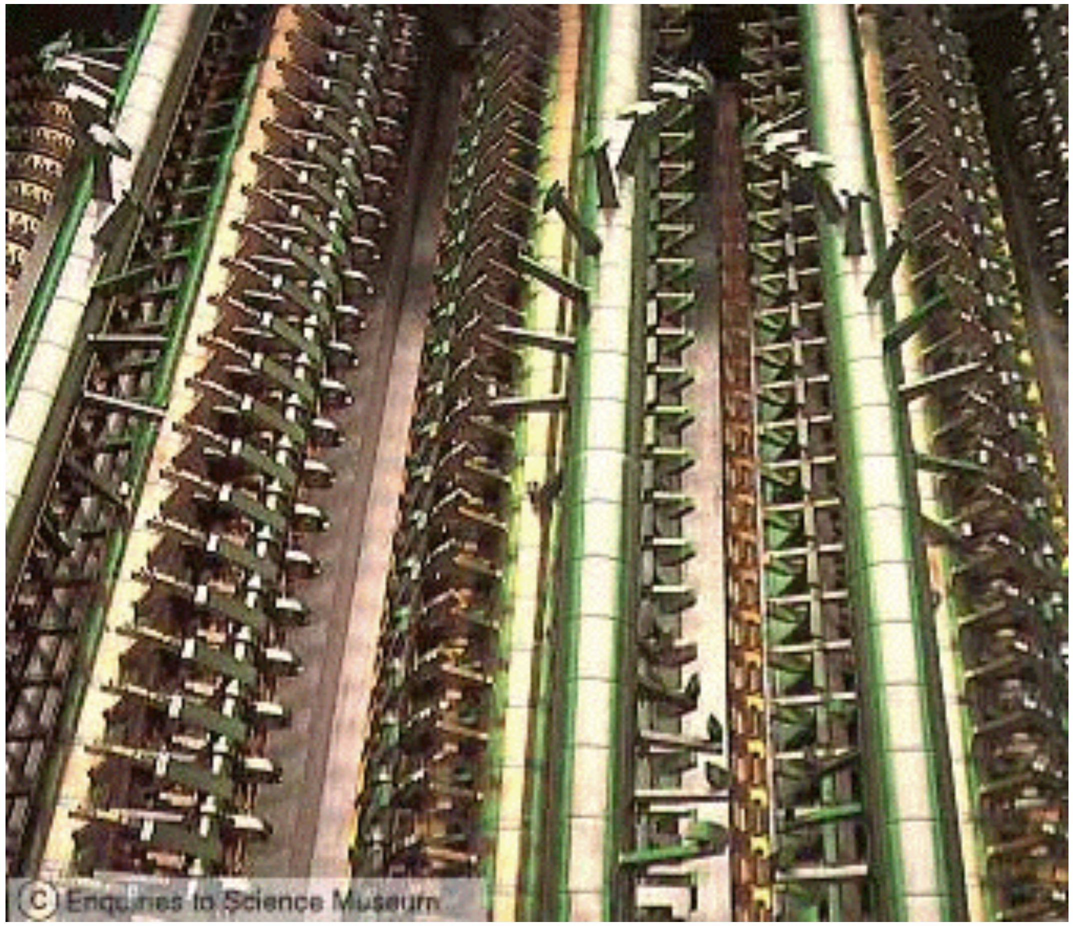
This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manu-facturing error, and probably will not work.



inappropriate hardware

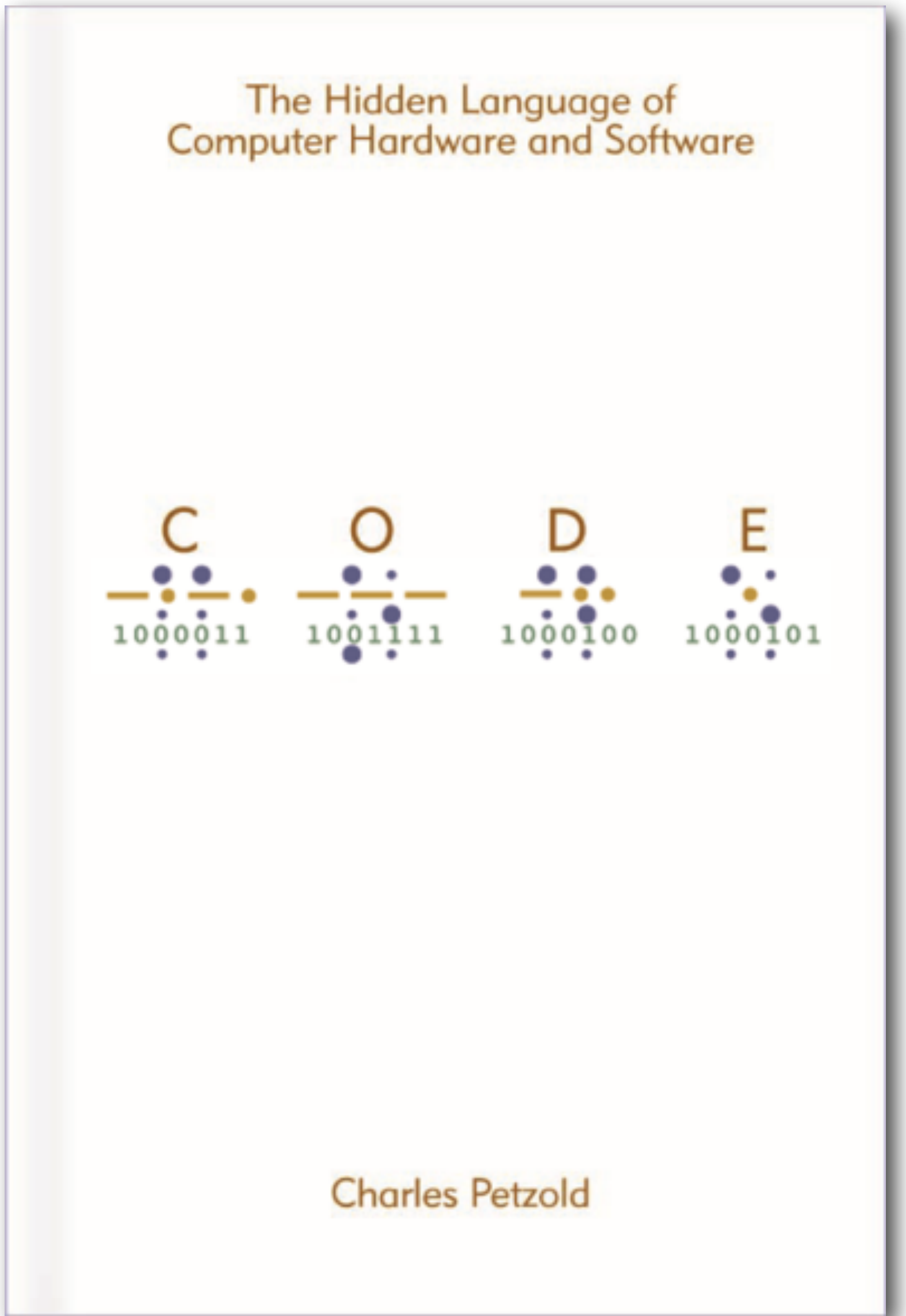
mechanical computers



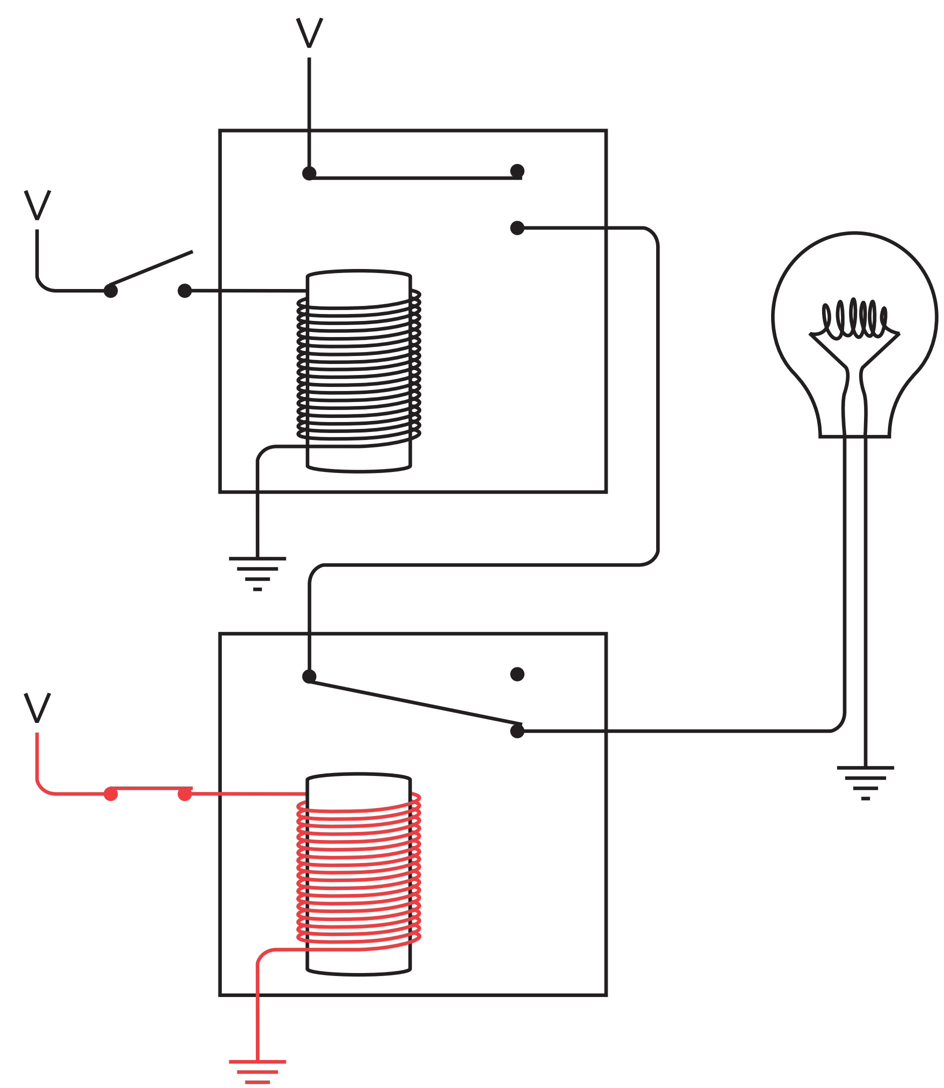


Charles Babbage: Analytical Engine (1834)

how to build a computer from relais



Charles Petzold: **Code**
The Hidden Language of
Computer Hardware and Software
Microsoft Press, 2000



Quantum Cryptography

MagiQ: www.magiqtech.com
id quantique: www.idquantique.com

Figure 3: id Quantique's system exchanged keys over 67 km of standard optical fiber.

Confused?

Möglicherweise ist es, nebenbei gesagt, für die Kopenhagener Interpretation der Quantenmechanik wichtig, dass ihre Sprache in einem gewissen Grad unbestimmt ist, und ich bezweifle, dass sie durch den Versuch, diese Unbestimmtheit zu vermeiden, klarer werden kann. (W. Heisenberg)